

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

**Defendants' Motion For Evidentiary Hearing and to Suppress All Evidence Seized
Pursuant to Unreasonably Executed Search Warrants
With Incorporated Memorandum of Law**

Now come the Defendants, Chenguang Gong and Yalan Tang, by and through undersigned counsel, pursuant to the Fourth Amendment, and hereby move the Court for an order suppressing any and all evidence seized pursuant to three search warrants authorizing seizure of an email account and electronic devices, to the extent the Court concludes, after an evidentiary hearing, that the government’s execution of the subject warrants violates the Fourth Amendment. *See, e.g. Dalia v. United States*, 441 U.S. 238, 258 (1979) (“the manner in which a warrant is executed is subject to later judicial review as to its reasonableness”); *United States v. Ganias*, 824 F.3d 199, 209-10 (2d Cir. 2016) (“both the scope of a seizure permitted by a warrant, and the reasonableness of government conduct in executing a valid warrant, can present Fourth Amendment issues”). Here, the government seized the entirety of an email database more than 30 months ago (in April 2019), and it seized twenty-one electronic devices from the defendants’ residence in November 2020, yet it concedes that (1) it has not yet completed the filtering process compelled by the controlling search warrants, much less its review of the email materials, and (2) it has not yet even begun a “systemic review” of the computer images that remain in its possession.

“As the text [of the Fourth Amendment] makes clear, ‘the ultimate touchstone of the Fourth Amendment is ‘reasonableness.’” *Riley v. California*, 573 U.S. 373, 381–82 (2014) quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006). As such, while some courts have observed—in different circumstances, and in response to different arguments than presented here—that the Fourth Amendment “contains no requirements about when [a] search or seizure is to occur or its duration,” *United States v. Syphers*, 426 F.3d 461, 469 (1st Cir. 2005), it indisputably does demand *reasonableness*. *See, e.g. United States v. Metter*, 860 F. Supp. 2d 205, 215 (E.D.N.Y. 2012) (Fourth Amendment “requires the government to complete its review, *i.e.*, execute the warrant, within a ‘reasonable’ period of time,”, and “the manner in which the government executes the warrant must comport with the Fourth Amendment’s reasonableness standard”).

Here, the government seized a massive quantity of electronic evidence capable of holding “the most intimate details of one’s life,” yet virtually the entirety of that evidence remains subject to on-going government examination—clearly a “substantial intrusion upon [Defendants’] personal privacy and dignity.” *United States v. Cotterman*, 709 F.3d 952, 968 (9th Cir. 2013); *see also United States v. Kolsuz*, 890 F.3d 133, 145 (4th Cir. 2018), as amended (May 18, 2018) (noting that the “average 400–gigabyte laptop hard drive can store over 200 million pages,” and that “[s]ubjected to comprehensive forensic analysis, a digital device can reveal an unparalleled breadth of private information”). The defendants respectfully submit an evidentiary hearing is needed to determine the exact circumstances surrounding the search process employed in this case, so the Court can engage in a careful, case-specific factual analysis and ultimately determine whether the government’s conduct comports with the Fourth Amendment. *See United States v. Filippi*, 2015 WL 5789846, at *8 (N.D.N.Y. Sept. 9, 2015)

(noting “‘there is no established upper limit as to when the government must review seized electronic data to determine whether the evidence seized falls within the scope of a warrant,’ and the issue ‘requires a careful case-by-case factual analysis because what may be appropriate under one set of facts and circumstances may not be so under another’”) (*quoting Metter*, 860 F. Supp. 2d at 215).

Should the Court, after such an inquiry, find the search process employed in this case violates the Fourth Amendment, the defendants respectfully submit that any and all evidence seized pursuant to the unreasonable executions must be suppressed, as well as all evidence deriving therefrom. *See, e.g., Murray v. United States*, 487 U.S. 533, 536-37 (1988); *Wong Sun v. United States*, 371 U.S. 471, 487-488 (1963)

Local Rule 7.1(a)(2) Certification

The parties have conferred and the government has advised it will oppose the relief sought herein.

Memorandum of Law

I. Relevant Factual Background.

As detailed in the following table, the government secured three warrants in this case authorizing the seizure of electronic evidence:

DATE	SEARCH WARRANT	RETURN
3/25/19	Search Warrant for the contents of the e-mail account known as info@ycells.com , including the content of all emails available to the electronic service provider, Endurance International Group, Inc. (“Endurance,” herein)	On April 10, 2019, the government secured a computer disc containing all responsive materials, including emails totaling approximately 30,000 pages, ranging in dates from February 2016, to March 27, 2019.

	(“Email Search Warrant No.1”, herein)	
11/9/2020	Search Warrant for the Gong/Tang residence, located at 284 Lake Street, Belmont, Massachusetts (“Gong/Tang Residence Search Warrant,” herein).	Warrant executed on November 10, 2020, with officers seizing, <i>inter alia</i> , twenty-one (21) different electronic devices.
2/8/21	A second Search Warrant for the contents of the e-mail account known as info@ycells.com , including the content of all emails available to Endurance dated from March 25, 2019 to November 10, 2020 (“Email Search Warrant No.2”, herein). ¹	Warrant served on Endurance on February 9, 2021, responsive materials produced to the government on March 4, 2021, including approximately 30 emails dated in March 2019. ²

Attachment B to the email search warrants sets forth the controlling search protocol. It compels Endurance to provide the government with a duplicate of the entire email account, and it then authorizes the government to “search the account duplicate for the records and data to be seized,” which is described in Section III of Attachment B. *See* Attachment B, Email Search Warrant No. 1, at Section I; Attachment B, Email Search Warrant No. 2, at Section I. Likewise, Attachment B of the search warrant for the Gong/Tang residence authorized the seizure of all computer

¹ Email Search Warrant No. 1 (with Attachments A and B) and the Return are attached hereto as Exhibit 1, the Gong Residence Search Warrant (with Attachments A and B) and the Inventory of Return (for the computers) are attached hereto as Exhibit 2, and Email Search Warrant No. 2 (with Attachments A and B) and the Return are attached hereto as Exhibit 3. The search warrant affidavits are being offered to the Court under seal pursuant to a contemporaneous motion to seal.

² YCells LLC is a Massachusetts based corporation. In his affidavit in support of the first search warrant for the emails, Agent Hughes averred that the Commonwealth’s Division of Corporation records listed Yalan Tang as the Resident Agent for YCells LLC when it was incorporated. *See, e.g.*, Hughes Affidavit in Support of First Email Warrant at ¶19. Additionally, the records produced by Endurance International Group lists Yalan Tang for the email account contact information. *See* Bates 00000002, 005.

hardware, computer software and storage media found within the home, but it further provided that any “off-site searching of these items shall be limited to searching for items described in Paragraph I.” Attachment B, Gong/Tang Residence Search Warrant, at Section II. Paragraph I, in turn, defines the items to be seized.

On December 6, 2021, counsel for the defendants wrote an email to government counsel requesting certain details regarding execution of the search warrants for electronic materials, in particular the dates each search began, the dates each search ended, and what if any search protocols were used in examining the relevant materials. The government responded via email on December 7, 2021, as follows:

The Government received the returns from the March 25, 2019 search warrant for content related to the email account info@ycells.com on [April] 10, 2019. Shortly after, the returns were uploaded to a searchable government data[base] by FDA agents. Subsequently, the returns were also uploaded to a []searchable database maintained by the U.S. Attorney’s Office. Since that time, the Government has searched for documents responsive to Attachment B to the warrant using search terms and other methods and anticipates continuing to do so.

As to the electronic devices seized on November 12, 2020 (and identified on the Inventory of Evidence produced as Bates Nos. Gong-Tang_30656 - Gong-Tang_30658): Item Nos. 6, 11, 15 and 16 were previewed by the Government and determined not to have relevant materials. These items were not imaged and were returned to your clients. The Government has been unable to access the contents of Item Nos. 1 and 12 and has retained those devices. Between November 12, 2020 and December 20, 2020, the Government created forensic images of the remaining devices. These devices have been returned to your clients.

At this time, the Government has not undertaken a systematic review of the contents of these devices. The Government anticipates that it will continue to review the contents of these devices for material responsive to Attachment B of the November 9, 2020 search warrant.

On December 15, defense counsel wrote government counsel once again to confirm their understanding of the search process employed to date; *i.e.*, that (1) “there was no filtering process before the emails were uploaded” to the government’s searchable databases, “but instead

all of the seized emails have been uploaded” to the government’s databases; and (2) for the computer devices that remain in the government’s possession and subject to continued review, “there has been no filtering process and the entirety of the devices within [the government’s] possession remain available” to the government. The government confirmed that the Defendants’ understanding was correct.

II. An evidentiary hearing should be convened to examine the reasonableness of the government’s execution of the subject search warrants.

“The general touchstone of reasonableness which governs Fourth Amendment analysis ... governs the method of execution of the warrant.” *United States v. Ramirez*, 523 U.S. 65, 71 (1998) (internal citation omitted); *see also Ganias*, 824 F.3d at 209-10 (“both the scope of a seizure permitted by a warrant, and the reasonableness of government conduct in executing a valid warrant, can present Fourth Amendment issues”). A “seizure lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution unreasonably infringes possessory interests protected by the Fourth Amendment’s prohibition on ‘unreasonable seizures.’” *United States v. Jacobsen*, 466 U.S. 109, 124 (1984); *see also United States v. Alvarez-Tejeda*, 491 F.3d 1013, 1016 (9th Cir. 2007) (“An otherwise lawful seizure can violate the Fourth Amendment if it is executed in an unreasonable manner”). Indeed, the Supreme Court has held that “the manner in which a warrant is executed is subject to later judicial review as to its reasonableness.” *Dalia*, 441 U.S. 258.

An issue that has emerged in our technological age, and which demands further scrutiny from the courts, is what constitutional constraints exist, and what constitutional protections remain, *after* the government executes a search warrant authorizing the wholesale seizure of computer equipment and electronic evidence—seizures which necessarily include materials well

outside the scope of the warrant. As early as 1976, the Supreme Court cautioned against searches of documents given the privacy risks attendant to such searches:

We recognize that there are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable. In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.... *In [these] kinds of searches, responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.*

Andresen v. Maryland, 427 U.S. 463, 482, n. 11 (1976) (emphasis added). The potential for “unwarranted intrusions” into a citizen’s privacy, and the corresponding need for the acute attention of responsible judicial officials, have been immeasurably amplified by the technological advances since the Court issued this warning more than 40 years ago. *See Matter of Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 157, 162–68 (D.D.C. 2014) (“it is certainly true that searches for electronic data may present increased risks to the individual’s right to privacy as technological advances enable law enforcement to monitor and collect large volumes of electronic communications and other data”). Indeed, given the vast storage capabilities of the modern computer, the government’s wholesale seizures of computer equipment and email accounts inevitably results in the seizure of evidence entirely outside the parameters of any controlling search warrant. *See United States v. Schesso*, 730 F.3d 1040, 1042 (9th Cir. 2013) (“Because electronic devices could contain vast quantities of intermingled information, raising the risks inherent in over-seizing data ... law enforcement and judicial officers must be especially cognizant of privacy risks when drafting and executing search warrants for electronic evidence”).

This constitutional concern is precisely why Attachments B to the subject search warrants set forth a two-step process. Law enforcement officers were required, by the very terms of the

email warrants, to search the electronic evidence “for the records and data to be seized,” as described in Section III of Attachment B. *See* Exhibits 1 and 3. Likewise, the Gong/Tang Residence Search Warrant specified that any off-site searching of computers taken from the home “shall be limited to searching for the items described in paragraph I” of the Attachment B. *See* Exhibit 2. It appears, however, the government ignored these express limitations. Instead, the government executed a search warrant for the Gong/Tang residence and seized every piece of computer equipment and device it observed, seemingly without any discrimination or examination. It likewise secured the contents of an entire email account, dating all the way back to January 1, 2014, and then received additional authorization to secure the contents of the same email account for the period March 25, 2019 to November 10, 2020. Thereafter, notwithstanding the grave and indisputable privacy concerns implicated by these vast seizures (as well as the plain language of the warrants themselves), the government to this day retains unfettered access to the entirety of the seized email accounts and all of the computer images that remain in the government’s possession, and the government apparently believes it is authorized to indefinitely peruse these materials, at its leisure, without any filtering process and without any active judicial oversight. This process would be anathema to the Framers and, the defendants respectfully submit, it demands an evidentiary hearing to determine exactly what the process has entailed in this case and whether it comports with the Fourth Amendment.

In *United States v. Aboshady*, 951 F.3d 1 (1st Cir.2020), the First Circuit recently rejected a challenge to the government’s execution of a search warrant for emails held by Google, but the claims raised in that case were different than those raised herein. There, the defendant argued the government’s execution violated the warrant because, “in preparation for trial, [the government] retained all of the data [turned over by Google] and possibly searched it”

Aboshady, 951 F.3d at 5. The First Circuit noted that “Aboshady appears to premise this contention on an assertion that the warrant did not permit the government to retain for as long as it did either his personal emails or any of the other electronic documents contained within the data that the government had acquired from Google, Inc,” and he “appears to contend that the warrant did not permit the government to then search the personal information contained in the emails and the electronic documents to which he refers.” *Aboshady*, 951 F.3d at 5. The Court first held that the government’s creation of a searchable database did not violate the search warrant, *Aboshady*, 951 F.3d at 5, a claim that is not made here. The Court then held that nothing within the warrant “set[] forth a time limit on retention of the data that Section II plainly authorized the government to acquire from Google, Inc.” and that, “given the absence of any such time limit, we do not see why it would be unreasonable to interpret the warrant to permit the government to retain that data until the appeals are completed.” *Aboshady*, 951 F.3d at 7. Lastly, the Court held that “[t]o the extent that Aboshady means to argue that the government’s execution of the warrant flagrantly violated its terms because the government not only retained the data that it had acquired from Google, Inc. pursuant to Section II of the warrant but also may have run searches on that data for years afterwards ‘as it developed new theories’ of his possible criminal liability, we are also not persuaded.” *Aboshady*, 951 F.3d at 7. The Court noted that “an ‘unreasonable delay’ in conducting a search that had been authorized by a warrant could ‘result [] in the lapse of probable cause,’ but there is no evidence in the record here that suffices to show that probable cause had lapsed at the time that any particular search of the data may have been conducted.” *Aboshady*, 951 F.3d at 7 (internal citations omitted).

Aboshady does not control here, as it is a decision rooted in the terms of the search warrant issued in that case and the particular process employed in that case. In *Aboshady*, it

appears the government actually engaged in the filtering process compelled by the search warrants, and it was performed by FBI personnel who were not part of the prosecution team.

United States v. Aboshady, 2017 WL 4540958, at *2 (D. Mass. Oct. 11, 2017) (Bowler, U.S.M.J.), *objections overruled*, 297 F. Supp. 3d 232 (D. Mass. 2018), *aff'd*, 951 F.3d 1 (1st Cir. 2020) (“Here, the government engaged in a two-step process sanctioned under Fed.R.Crim.P. 41(e)(2)(B) (“Rule 41(e)(2)”). *See U.S. v. Kanodia*, 2016 WL 3166370, at *6-7 (D. Mass. June 6, 2016). Under the first step, the government executed the warrants on Google and AOL, and FBI personnel received the electronic data. In order to review the material via-à-vis the second step, FBI personnel uploaded the estimated 430,081 documents received into a searchable database and applied search terms to filter out potentially privileged communications, including the name and the e-mail address of the defendant’s attorney. The FBI personnel engaged in the foregoing ‘were not part of the prosecution team.’”) (internal docket citations omitted). That does not appear to be the case here. Moreover, the Magistrate Judge in *Aboshady* concluded that, similar “to the circumstances in *Upham*, the seizure of all electronic data associated with the e-mail accounts and the subsequent uploading, application of search terms, and search of the data ‘was about the narrowest definable search and seizure reasonably likely to obtain’ the targeted information.” *Aboshady*, 2017 WL 4540958, at *2 (D. Mass. Oct. 11, 2017) (Bowler, U.S.M.J.), *objections overruled*, 297 F. Supp. 3d 232 (D. Mass. 2018), *aff'd*, 951 F.3d 1 (1st Cir. 2020), quoting *United States v. Upham*, 168 F.3d 532, 535 (1st Cir.1999). Whether or not the “government” writ large may permissibly retain the entire email database so there is a complete record pending appeals, neither *Aboshady* nor the search warrants issued in this case should be viewed as permitting the government prosecutorial team to ignore a warrant’s command to filter

responsive from unresponsive, and/or to indefinitely possess materials outside the scope of the search warrants.

Likewise, the First Circuit’s refusal to categorically prohibit the possibility of searches on seized email data “for years afterwards” does not resolve the claims pressed here. First, Aboshady appeared to “argue that the government’s execution of the warrant flagrantly violated its terms,” but the defendants here contend that the government’s failure to reasonably execute the subject warrants runs afoul of the *Fourth Amendment*, not simply the search warrants. Secondly, Aboshady apparently argued there was a possibility the government may have run additional searches on the data set for years afterwards, when probable cause may have lapsed, but the issue here, at this point, is not whether the government could conceivably go back to the original dataset if a new theory emerged. Instead, the issue presented here is whether the government’s failure to conduct an initial filtering review of the email database for thirty-plus months after issuance of the warrant, its failure to even begin a “systemic review” of the computer images that remain in its possession, and its undefined and ongoing searches of the databases despite such a failure to properly filter, comports with the Fourth Amendment. Indeed, the search in *Aboshady* consisted of more than 400,000 *emails*, *United States v. Aboshady*, 297 F. Supp. 3d 232, 235 (D. Mass. 2018), *aff’d*, 951 F.3d 1 (1st Cir. 2020), while the email seizure here numbers around 30,000 *pages*, so whatever durational time may have been permissible in *Aboshady* may not be reasonable here. And, of course, whether or not a search and seizure violates the Fourth Amendment necessarily depends on the specific facts of the particular case at issue. Finally, it bears noting that although denying defendant’s claims in *Aboshady*, Judge Gorton issued the following warning to the government, or “necessary caveat,” in the court’s words:

The warrant process “is primarily concerned with identifying what may be search or seized—not how,” *United States v. Upham*, 168 F3d at 537. The government’s contention that it may therefore indefinitely hold electronic information for subsequent searches threatens, however, to breach the reasonableness requirement. The issue arises from the intersection of the Fourth Amendment’s particularity requirement and its prohibition on unreasonable searches. A warrant must 1) limit the executing agent’s “judgment in selecting where to search and what to seize” and 2) cannot be so broad as to include “items that should not be seized.” *United States v. Kuc*, 737 F.3d 129, 133 (1st Cir.2013) (*citing United States v. Upham*, 168 F.3d 532, 535 (1st Cir.1999)). Some courts have suggested that, because of the “nature of digital storage, it is not always feasible to extract and segregate responsive data from non-responsive data.” *United States v. Ulbricht*, 858 F.3d 71, 99-100 (2d Cir.2017). Nevertheless, reasonableness requires that searches and seizures by the government be “conducted in a manner that minimizes unwarranted intrusions upon privacy.” *Andreson v. Maryland*, 427 U.S. 463, 482 n.11 (1976). Although defendant’s request for suppression *in this particular case and under these particular circumstances* will be denied, *the government’s continued responsibility to minimize the extent and duration of digital discovery is not abrogated*.

Aboshady, 297 F.Supp.3d at 239 (emphasis added).

The defendants respectfully submit that, as the court held in *United States v. Metter*, 860 F. Supp. 2d 205, 215 (E.D.N.Y. 2012), the Fourth Amendment “requires the government to complete its review, *i.e.*, execute the warrant, within a ‘reasonable’ period of time,” and “the manner in which the government executes the warrant must comport with the Fourth Amendment’s reasonableness standard,” *id.* at 212-13. The government must not be permitted to seize a citizen’s most private possessions and papers and peruse them indefinitely, at the very least not without a meaningful inquiry into the process, so the Court can actually ensure that the process employed in the particular case at issue comports with the Fourth Amendment. *See In the Matter of a Warrant for All Content and Other Information Associated With the Email Account XXXX@gmail.com*, 33 F.Supp.3d at 396 (“*Dalia* held that ‘the manner in which a warrant is executed is subject to later judicial review as to its reasonableness’”); *id.* at 396-97 (“*Grubbs* held that the Constitution “interpos[es], *ex ante*, the deliberate, impartial judgment of a

judicial officer” and provides “*ex post*, a right to suppress evidence improperly obtained and a cause of action for damages” for an unreasonable search).

III. Conclusion.

Here, the defendants respectfully submit that the conduct at issue—government agents seizing the entirety of an email database and multiple computers, and then retaining the unfettered ability to rummage through these huge repositories of information, without any meaningful judicial oversight or accounting, for an indefinite period of time—is the present day analog to the general warrants “abhorred by the colonists” and which served as the foundation of the Fourth Amendment. *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971); *see also Metter*, 860 F. Supp. 2d at 212 (holding “government’s more than fifteen-month delay in reviewing the seized electronic evidence, under the facts and circumstances of th[at] case, constitute[d] an unreasonable seizure under the Fourth Amendment”).

As such, for all of the foregoing reasons, the defense respectfully submits that an evidentiary hearing must be convened to examine the precise circumstances surrounding the government’s execution of the subject search warrants—*i.e.*, what has the government done to date with the electronic materials, who has access to them, what filtering process has been executed, and why has the government not yet completed the searches compelled by the warrants. *See Warshak v. United States*, 532 F.3d 521, 528 (6th Cir. 2008) (*en banc*) (in determining “reasonableness” of searches under the Fourth Amendment, “reviewing court looks at the claim … in the context of a developed factual record” because the Fourth Amendment “generally should be applied after [factual] circumstances unfold, not before”). Only then can the Court conduct the “careful” and “factual” analysis required to determine whether the government’s execution of the warrants in this case comported with the Fourth Amendment.

United States v. Filippi, 2015 WL 5789846, at *8 (N.D.N.Y. Sept. 9, 2015) (“For this reason, ‘there is no established upper limit as to when the government must review seized electronic data to determine whether the evidence seized falls within the scope of a warrant,’ and the issue ‘requires a careful case-by-case factual analysis because what may be appropriate under one set of facts and circumstances may not be so under another’”) (*quoting Metter*, 860 F.Supp.2d at 215). To the extent the government’s execution of the search warrants violated the Fourth Amendment, the Court should suppress any and all evidence infected by the constitutional violations.

Respectfully Submitted,
The Defendant,
Chenguang Gong,
By His Attorney,

/s/ Robert M. Goldstein
Robert M. Goldstein
20 Park Plaza, Suite 1000
Boston, MA 02116
(617) 742-9015
rmg@goldstein-lawfirm.com

Respectfully Submitted,
The Defendant,
Yalan Tang,
By Her Attorney,

/s/ Douglas S. Brooks
Douglas S. Brooks
Libby Hoopes Brooks, P.C.
399 Boylston Street
Boston, MA 02116
(617) 338-9300
dbrooks@lhblaw.com

Certificate of Service

I, Robert M. Goldstein, hereby certify that on this date, December 17, 2021, a copy of the foregoing document has been served via the Electronic Court Filing system on all registered participants, including Assistant U.S. Attorney Chris Looney.

/s/ Robert M. Goldstein
Robert M. Goldstein